IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. 09/210,213
Inventorship ..... LaPorta
Filing Date ..... December 11, 1998
Assignee ..... Lucent Technologies Inc.
Art Unit 2663
Examiner ..... Duc T. Duong
Docket No. ..... La Porta 42-6-13-3-4
Customer No. 50959
Title: Single Phase Local Mobility Scheme for Wireless Access to Packet-Based Networks

AFFIDAVIT UNDER C.F.R. 1.131
AFFIDAVIT OF RAMACHANDRAN RAMJEE

State of New Jersey
County of Union

To the Commissioner of Patents:

being duly sworn, deposes and says:

1. I am a named inventor of Application No.09/210,213, relating to methods for wireless access to packet based networks by mobile devices, and on December 11, 1998 filed the above-identified application.

2. I conceived of the invention in this country on March 9, 1998.

3. I kept records of the progress while working thereon with others at Lucent Technologies, namely, Thomas F. LaPorta (no longer with Lucent Technologies), Kazutaka Murakami, Sandra Thuel, and Kannan Varadhan (no longer with Lucent Technologies). Photostatic copies of records are attached hereto as exhibits.

Records (exhibits) include:

i. notes on the invention dated January 13, 1998
ii. computer records in support of the invention (a domain-based approach for supporting mobility in wireless networks) dated March 9, 1998
iii. computer records to demonstrate continued diligence from a time prior to the effective date of the cited reference to a subsequent filing of the application. (computer documents are dated beginning March 9, 1998)
iv. text documents that were written prior to May 12, 1998 demonstrating that the invention was conceived of prior to the effective date of the cited reference.

4. On information and belief I state that the invention or any claim thereof was not on sale or in public use in this country, nor was it patented or described in a printed publication in this or a foreign country, more than one year prior to the date of the above identified application for patent or the filing date of the application for Patent No. 6,473,411, which substantially shows or describes but does not claim my invention, which was filed on May 12, 1998.

5. My invention has never been abandoned.

R. Ramjee

Ramachandran Ramjee

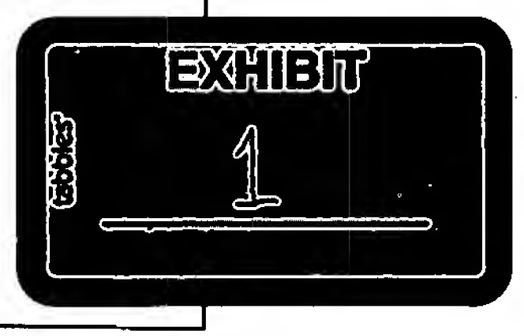
On this 27th day of November, 2006, before me personally came Ramachandran Ramjee, known to be the individual described in and who executed the foregoing instrument, and acknowledged execution of the same.

Darlene McDougald

Notary Public

DARLENE McDOUGALD
NOTARY PUBLIC OF NEW JERSEY
My Commission Expires Aug. 6, 2008

```
total 6192
-rw-r--r--   1 ramjee   ramjee      8628 Mar  9  1998 .~hawaii.1
-rw-r--r--   1 ramjee   ramjee       833 Apr 28  1998 .~hawaii_mob
-rw-r--r--   1 ramjee   ramjee      4993 May  6  1998 .~hawaii_mob.2
-rw-r--r--   1 ramjee   ramjee      2041 Aug 28  1998 .~tcpnew.out
-rw-rw-rw-   1 ramjee   ramjee     13217 Sep 24  1998 .~hawaii.tex
-rw-r--r--   1 ramjee   ramjee   1014953 Nov 12  1998 arch.doc
-rw-r--r--   1 ramjee   ramjee       740 Nov 17  1998 .~enddevice.1
-rw-r--r--   1 ramjee   ramjee       745 Nov 17  1998 enddevice.1
-rw-r--r--   1 ramjee   ramjee   1254750 Jan  7  1999 hmip.ps
-rw-r--r--   1 ramjee   ramjee      1623 Nov 11  1999 ietf.2-
-rw-r--r--   1 ramjee   ramjee      2246 Nov 11  1999 ietf.2
-rw-r--r--   1 ramjee   ramjee      8106 Nov 14  1999 hawcell.txt
-rw-------   1 ramjee   ramjee     10612 Nov 15  1999 ram.1
-rw-r--r--   1 ramjee   ramjee      1445 Mar 15  2000 softhandoff
-rw-r--r--   1 ramjee   ramjee      2621 Mar 15  2000 privateaddress
drwxr-xr-x  11 ramjee   ramjee      4096 Jan  5  2001 paging/
-rw-r--r--   1 ramjee   ramjee    757760 Mar 15  2001 hawaii-src.tar
drwxr-xr-x  12 ramjee   ramjee      4096 Sep 27  2004 ../
drwxr-xr-x   2 ramjee   ramjee      8192 Jan 31  2006 rfc/
drwxr-xr-x   8 ramjee   ramjee      4096 Jan 31  2006 sim/
drwxr-xr-x  16 ramjee   ramjee      4096 Jan 31  2006 impl/
drwxr-xr-x  13 ramjee   ramjee      8192 Jan 31  2006 doc/
drwxr-xr-x   7 ramjee   ramjee      4096 Nov 10 15:31 ./
-rw-r--r--   1 ramjee   ramjee         0 Nov 10 15:31 dir.txt
```



```
total 22344
-rw-r--r--   1 ramjee   ramjee     13280 Mar  9  1998 k.rep
-rw-r--r--   1 ramjee   ramjee      8724 Mar 27  1998 hawaii.1
-rw-r--r--   1 ramjee   ramjee      4099 Apr 30  1998 hawaii_mob
-rw-------   1 ramjee   ramjee      4993 Apr 30  1998 hawaii_mob.1
-rw-r--r--   1 ramjee   ramjee      9173 May  6  1998 hawaii_mob.2
-rw-r--r--   1 ramjee   ramjee       841 May 14  1998 hawaii.benefits
-rw-r--r--   1 ramjee   ramjee     46782 Oct 12  1998 hawaiitmp.tex
-rw-r--r--   1 ramjee   ramjee     50906 Oct 29  1998 hawaii.tex
-rw-r--r--   1 ramjee   ramjee         0 Dec 22  1998 hawaii.ps
-rw-r--r--   1 ramjee   ramjee      1846 Dec 23  1998 hawaii3.log
-rw-r--r--   1 ramjee   ramjee     84964 Dec 23  1998 hawaii3.dvi
-rw-r--r--   1 ramjee   ramjee      5977 Dec 23  1998 hawaii3.aux
-rw-r--r--   1 ramjee   ramjee    269258 Dec 23  1998 hawaii3.ps
-rwxr-xr-x   1 ramjee   ramjee     86532 Dec 23  1998 hawaii3.tex*
-rw-r--r--   1 ramjee   ramjee      6243 Jan 22  1999 hawaii.log
-rw-r--r--   1 ramjee   ramjee     63876 Jan 22  1999 hawaii.dvi
-rw-r--r--   1 ramjee   ramjee      5267 Jan 22  1999 hawaii.aux
-rw-r--r--   1 ramjee   ramjee   1658006 Jan 26  1999 hw.ps
-rw-rw-rw-   1 ramjee   ramjee     95541 Jan 27  1999 hawaii4.old.tex
-rw-r--r--   1 ramjee   ramjee   1600532 Jan 28  1999 hawaii4.ps
-rw-rw-rw-   1 ramjee   ramjee    102710 Jan 28  1999 hawaii4.tex
-rw-r--r--   1 ramjee   ramjee      5946 Jan 28  1999 hawaii4.log
-rw-r--r--   1 ramjee   ramjee    119616 Jan 28  1999 hawaii4.dvi
-rw-r--r--   1 ramjee   ramjee      6961 Jan 28  1999 hawaii4.aux
-rw-rw-rw-   1 ramjee   ramjee    113823 Feb  2  1999 hawaii5.tex
-rw-r--r--   1 ramjee   ramjee      6824 Feb  2  1999 hawaii5.aux
-rw-r--r--   1 ramjee   ramjee    121876 Feb  2  1999 hawaii5.dvi
-rw-r--r--   1 ramjee   ramjee   1633413 Feb  2  1999 hawaii5.ps
-rw-r--r--   1 ramjee   ramjee      2832 Feb  2  1999 hawaii5.log
-rw-r--r--   1 ramjee   ramjee      6843 Feb  3  1999 hawaii6.aux
-rw-r--r--   1 ramjee   ramjee    124736 Feb  3  1999 hawaii6.dvi
-rw-r--r--   1 ramjee   ramjee   1638288 Feb  3  1999 hawaii6.ps
-rw-r--r--   1 ramjee   ramjee      2997 Feb  4  1999 hawaii6.log
-rw-rw-rw-   1 ramjee   ramjee    115799 Feb  4  1999 hawaii6.tex
-rw-r--r--   1 ramjee   ramjee    117136 Feb 18  1999 hawaii7.tex
-rw-r--r--   1 ramjee   ramjee      5611 Feb 18  1999 hawaii7.log
-rw-r--r--   1 ramjee   ramjee    126212 Feb 18  1999 hawaii7.dvi
-rw-r--r--   1 ramjee   ramjee      7130 Feb 18  1999 hawaii7.aux
-rw-r--r--   1 ramjee   ramjee   1632150 Feb 18  1999 hawaii7.ps
-rw-r--r--   1 ramjee   ramjee     62567 Feb 26  1999 fig1.latex.ps
-rw-r--r--   1 ramjee   ramjee      1901 Feb 26  1999 fig1.tex
-rw-r--r--   1 ramjee   ramjee      3798 Feb 26  1999 fig1.log
-rw-r--r--   1 ramjee   ramjee       292 Feb 26  1999 fig1.dvi
-rw-r--r--   1 ramjee   ramjee        35 Feb 26  1999 fig1.aux
-rw-r--r--   1 ramjee   ramjee     95854 Feb 26  1999 fig1.ps
-rw-r--r--   1 ramjee   ramjee     96002 Feb 26  1999 fig1.eps
-rw-r--r--   1 ramjee   ramjee      2837 Mar 19  1999 fig.tex
-rw-r--r--   1 ramjee   ramjee   1059026 Mar 19  1999 fig.ps
-rw-r--r--   1 ramjee   ramjee      4829 Apr 26  1999 fig.log
-rw-r--r--   1 ramjee   ramjee      2896 Apr 26  1999 fig.dvi
-rw-r--r--   1 ramjee   ramjee      1091 Apr 26  1999 fig.aux
drwxr-xr-x  13 ramjee   ramjee      8192 Jan 31  2006 ../
-rw-r--r--   1 ramjee   ramjee         0 Nov 10 15:35 dir2.txt
drwxr-xr-x   2 ramjee   ramjee      8192 Nov 10 15:35 ./
```

8/13

Goals '98

I Continuation of '97

- Batching, papers etc.
- DATA TRIAL, ASM, (10% or 50%)
- MSC SOFTWARE, PERF. MGMT (KAZU)
- SESS folks etc. (B.U. contract)

II New for '98

(DATA, 3rd Gen Wireless, Internet)

Agents

- Java proxies - allocation, scheduling, pricing, mobility (ACTIVE NETWORKING?)
- Base-station resource allocation, degradation (analytical)

Internet QoS

- Aggregate QoS (ELLEN)

III Resources: Summer student maybe...

Lab: ~~few~~ few Ultra-sparcs

Travel: conferences.

HAWAII: Hierarchical, Active, Wireless Access Internet Infrastructure

---

Philosophy: Same as the internet's- IP on end devices(phones/laptops), end devices query for services and control their use

What's New: Hierachical Mobility Management Architecture with Active Networking, Dynamic Frame Selection, Differentiated Services

Benefits: Active networking and Dynamic frame selection makes mobility management efficient, Benefits which are applicable in general to internet: scalability, robustness, faster deployment and richer set of services

Products: Wireless Enhanced Routers, Server software, Integration of several air interfaces

---

Details:

The infrastructure performs two main functions:

I) Mobility Management
II) Resource Allocation/Identification

At this juncture, I will present mostly the mobility management aspects of the architecture with some brief thoughts at the end on resource allocation/identification.

Notation: MS - Mobile Station, BS - Base-station

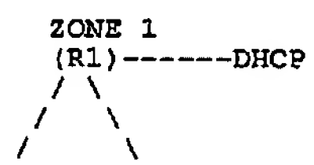
I) Mobility Management

We use a hierarchical mobility mangement architecture with two layers. At the top layer, we use mobileIP. We dynamically assign new IP addresses to MS when the MS enters new zones and update the home agent so that other hosts can contact the MS. At the bottom layer (within a zone), a handoff between two BSs result only in routing table updates in the appropriate routers in the zone - the MS's IP address is unchanged. In our architecture, the foreign agent of the mobileIP protocol is resident within the MS - thus, the home agent sends packets directly to the MS.

Also, every handoff within a zone results in a update of only a very localized set of routers and is done efficiently. Thus, there is no paging required. If this approach results in substantial overhead for users with high mobility_to_traffic ratios, one possibility is to track users at a higher granularity (for example, at the routers at the bottom-most level) and have the router coordinate paging. This option is not addressed currently.

Note that a zone is also a subnet. However, there are two differences between the zone and a typical subnet - 1) the zone is large subnet that is not further subdivided into smaller subnets 2) routers in the zone route packets based on full IP addresses of end devices (rather than just the network part of the IP addresses). The sizing of the zone will be based on many factors, such as router processing capacity, reliability needed, number of base-stations covered, number of IP addresses available for assignment etc.

Ia) Power up/down registration



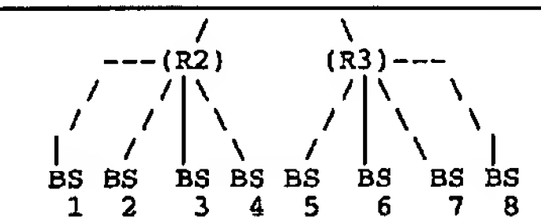


Figure 1

Figure 1 shows a typical zone (ZONE 1), with three routers and 8 BS. (for reliability, each BS/router can be connected to two or more routers).

For example, ZONE 1 might be subnet 135.180.xx.xx. This allows the assignment of ~65K addresses. Assuming ~60 MS's per BS, we will have about 1000 BS's in this zone.

The DHCP server, attached to R1, has a well known address, reachable from any of the BS (e.g.: 135.180.1.1). For load balancing and reliability purposes, it is possible to have multiple shared DHCP servers as per the DHCP standards.

Upon Power up registration, two activities are performed:

i) IP address assignment to Mobile Station (MS)

Let us assume MS sends a power up registration to BS4.

When BS4 receives the power up registration, it sends a message to the DHCP server, requesting IP address assignment for the given MS. The DHCP server performs authentication (with an HLR for example) and then chooses an available IP address, say, 135.180.100.1. It then sends this address as part of an ACTIVE MESSAGE to the BS4. All the routers in the path from the DHCP server to the BS4 will ADD A ROUTING TABLE ENTRY before forwarding the message - for example, R1 will add (135.180.100.1 -> R2) and R2 will add (135.180.100.1 -> BS4), while BS4 will have (135.180.100.1 -> air).

The BS finally informs the MS of the assigned IP address.

ii) Home agent update

The DHCP server (or the DHCP client running at the MS) contacts the home agent of the MS and informs it of the IP address (care-of-address) assigned to the MS.

At this point, the routers between the home agent and the mobile host have the necessary information to forward packets. Any correspondent host will send data packets to the home agent of the MS which then tunnels the packet to the MS (as per the MobileIP standard). The foreign agent is co-resident with the MS and decapsulates the packet.

Power down registration is analogous to power up registration.

Ib) Handoff within a zone

The IP address of the MS does not change within the zone. However, routing table entries of some of the routers in the zone will have to be changed so that packets destined to the MS will reach the new BS. We again use ACTIVE messages to change the routing table entries.

For example, let the MS handoff from BS4 to BS5 in Figure 1. When BS5 is notified of the handoff, it adds an entry (135.180.100.1 -> air) and sends an active message to BS4. This message updates the routing tables of all the routers in the path from BS5 to BS4 - R3 creates a new entry (135.180.100.1 -> BS5), R1 modifies its current entry to (135.180.100.1 -> R3) and R2 modifies its entry to a temporary entry

(135.180.100.1 -> R1). BS5 also modifies its entry to a temporary entry of the form (135.180.100.1 -> R2). The last two temporary entries (which will automatically expire after a certain timeout period) are needed for forwarding transient data from old BS, BS4, to new BS, BS5. Note that re-ordering of data is possible during handoff.

Note that the path of packets to the MS established by this procedure during a handoff may not be optimal - it will depend on the topology of the access network among other things. However, we expect that this handoff procedure will be close to optimal in most cases and is definitely very efficient.

Ic) Handoff across zones

Handoff across zones requires assignment of new IP address to the MS. This can be accomplished by an equivalent of a power up reg in the new zone and a power down registration in the old zone. Forwarding of data is accomplished in exactly the same way as in handoff within a zone.

II) Resource allocation/identification

Differentiated services:

Bandwidth reservations for implementing Quality of Service (QOS) can be provided through use of the differentiated services (diffserv) architecture. The zone will simply be a domain within the diffserv architecture and the (not-yet defined) mechanisms for supporting different QOS traffic classes in a diffserv domain can be reused (for example, mechanisms which negotiate bandwidth at the egress points of a domain will be applicable for the zone in our architecture).

Dynamic Frame Selection:

CDMA traffic requires frame selection functionality to select the best packet from the multiple packets received during soft handoffs. By implementing frame selection functionality into each of the routers in the zone, it might be possible to do dynamic frame selections - i.e., frame selectors need not be anchored for the duration of the call. During each soft handoff, an appropriate router is instructed by the BSs to perform the frame selection functionality. This results in more efficient routing of the call as well as distribution/load balancing of frame selection functionality among all the routers in the zone.

PPP service:

In the case of PPP service, the assignment of IP address will be done by the PPP server of the access provider. Each of the PPP control messages will have to be forwarded by the BS to the IWF which then contacts the PPP server. The IWF server in the zone will maintain an L2TP connection to the PPP server and an IP tunnel to the BS which then forwards packets to the MS.

PSTN gateway and other services:

The zone will provide a directory service to the MS, informing the MS of the location (IP address) of various servers. It is then upto the MS to directly negotiate with the servers. One could also imagine having user agents in the zone which do the negotiation on behalf of the MS.

Hello folks,

>
> Let's have our next meeting Tuesday May 5 at 10:30. Please send
> me any items you want to talk about so we can have a structured
> discussion. I would like to check our progress on the to do
> list plus come up with a list of technical problems that need to
> be solved such as:
> 1. mobility management (if 2 gateways)
> 2. FS selection (multiple flows, multiple gateways)
> I'm sure you all have others.
>
> Tom

I have made an outline of the technical issues involved in evaluation of the mobility management scheme of Hawaii. We will discuss these issues on tuesday. I have left out frame selection for the time being as it depends on the mobility management scheme. Comments/suggestions welcome.

Cheers,
Ram

---

1. Mobility Management

First, I have listed the salient features of Hawaii and four alternative proposals for mobility management. Then, I have listed several different criteria on which to compare these schemes.

2. Mobility Management Schemes

Note that all the schemes below use Mobile IP for macro-mobility management. The differences lie in how micro-mobility (handoff between cells) is managed.

Hawaii:

* Foreign Agent (FA) in Mobile Station (MS)

* When MS powers on, an active message update routers from Gateway Router (DHCP server) all the way to the Base Station (BS)

* Handoff is achieved by sending active messages between neighboring BS's

* Active router update messages are also sent periodically to refresh routing table entries

* We could send our active messages on multiple paths (multicast) to take multi-path forwarding into account (i.e., there are several equivalent paths between Gateway and BS or BS and BS).

(Alternative 1): have the FA in the Gateway router and use the MS's static address to route within the foreign access network - Q) Does this make sense?

Alternative Approaches:

1) Basic Mobile IP:

* The FA is in the BS, IP address (care-of address) changes on every handoff, update Home Agent (HA) on every move.

2) Hierarchical Foreign Agents:

* There are multiple FA's. For example, one in the Gateway (FA_G), and one in each BS (FA_BS). HA sends encapsulated packets to FA_G, which then sends encapsulated packets to FA_BS.

* IP address (care-of address) changes on every handoff, update FA_G on every move, update HA only when moving between FA_G's.

3) Flooding:

* FA is in MS

* On every handoff of the MS, broadcast the new location (BS) for the MS's assigned IP address throughout the foreign access network.

4) Multicasting:

* MS's current BS (and may be the neighboring BS's also) join a multicast group with the HA.

* As the MS moves, some BS's leave the group while others join the group.

(Alternative 1): Have FA in the gateway. Use basic Mobile IP between HA and FA. BS's join/leave multicast group with the FA.

3. Comparison Criteria

Issues	Hawaii	MIP	HFA	Flood	Mcast
1) Multiple Path Forwarding	C?	C	C	C	C
2) Signaling Message Loss	C	C	C	C	C
3) Security	C	C	C	C	C
4) Router failure	G?	G	G	G	G
5) FA failure	G^	G&	B	G	B^
6) IP address depletion	B^	G	G	B	G^
7) Wired Bandwidth overhead	VG#	B?	G	B	B
8) Disruption during handoff	G	B*	B*	B?	VG
9) Router processing overhead	B?	G?	G?	B?	B?
10) BS processing overhead	G?	G?	G?	B?	B?
11) Multicasting support	C	C	C?	C	C?
12) Looping/Fast movement handling	C?	C	C	C	C
13) Handoff Latency	VG?	B	G?	G?	VG
14) Quality of Service support(ease)	G?	B?	B?	G?	G?

Notes:

^: Depends on whether the alternative 1 suggested for these schemes is used
&: FA failure in MIP is equivalent to BS failure (which impacts all schemes)
#: If Frame-selection is used, wired bandwidth overhead will increase
*: Depends on whether we implement data forwarding from previous BS

QoS: Assuming that QoS support is difficult with encapsulated traffic

Rating:

VG: expected to be very good
G: expected to be good
B: expected to be below average
C: capable/supported

Hello folks,

Version 2 of the draft on mobility management schemes.
Comments/suggestions welcome.

Cheers,
Ram

---

1. Mobility Management

First, I have listed the salient features of Hawaii and four alternative proposals for mobility management. Then, I have listed several different criteria on which to compare these schemes.

2. Mobility Management Schemes

Note that all the schemes below use Mobile IP for macro-mobility management. The differences lie in how micro-mobility (handoff between cells) is managed.

Hawaii:

* Foreign Agent (FA) in Mobile Station (MS)

* When MS powers on, an active message update routers from Gateway Router (DHCP server) all the way to the Base Station (BS)

* Handoff is achieved by sending active messages between neighboring BS's

* Active router update messages are also sent periodically to refresh routing table entries

* We could send our active messages on multiple paths (multicast) to take multi-path forwarding into account (i.e., there are several equivalent paths between Gateway and BS or BS and BS).

(Alternative 1): have the FA in the Gateway router and use the MS's static address to route within the foreign access network - Q) Does this make sense?

Alternative Approaches:

1) Basic Mobile IP:

* The FA is in the BS, IP address (care-of address) changes on every handoff, update Home Agent (HA) on every move.

2) Hierarchical Foreign Agents:

* There are multiple FA's. For example, one in the Gateway (FA_G), and one in each BS (FA_BS). HA sends encapsulated packets to FA_G, which then sends encapsulated packets to FA_BS.

* IP address (care-of address) changes on e
on every move, update HA only when moving

3) Flooding:

* FA is in MS

* On every handoff of the MS, broadcast the new location (BS) for the MS's assigned IP address throughout the foreign access network.

4) Multicasting:

* MS's current BS (and may be the neighboring BS's also) join a multicast group with the HA.

* As the MS moves, some BS's leave the group while others join the group.

(Alternative 1): Have FA in the gateway. Use basic Mobile IP between HA and FA. BS's join/leave multicast group with the FA.

3. Comparison Criteria

Issues	HAWAII	MIP	HFA	FLOOD	MCAST
1) Handoff Latency	VG	VB	G	B	VG
2) Disruption during handoff	G	VB	B	B	VG
3) Wired Bandwidth overhead(control)	VG	B	G	VB	G
4) Wired Bandwidth overhead(data)	G	G	G	G	VB
5) Router processing overhead(control)	G	B	G	B	G
6) Router processing overhead(data)	B	G	B	B	VG
7) BS processing overhead(control)	G	G	G	B	B
8) BS processing overhead(data)	G	B	B	G	VB
9) Multiple Path Forwarding	C	C	C	C	C
10) Router failure	G	G	G	G	G
11) FA failure	G	G	B	G	B
12) IP address depletion	B	G	G	B	G
13) Signaling Message Loss	C	C	C	C	C
14) Security	C	C	C	C	C
15) Multicasting support	C	C	C	C	C
16) Looping/Fast movement handling	C	C	C	C	C
17) Quality of Service support(ease)	G	B	B	G	G

Rating:

VG: expected to be very good
G: expected to be good
B: expected to be bad
VB: expected to be very bad
C: capable/supported

Detailed Notes:

1) Handoff Latency:

High for MIP since HA needs to be updated.

Good for HFA since gateway FA is updated.
Very Good for MCAST,HAWAII - truly local updates (for example, nearest router).
FLOOD - do we count handoff complete as soon as MS joins new BS
or do we wait for the update flooding to complete?

2) Disruption during handoff

MIP and HFA - Very Bad/Bad, assuming we do not implement sophisticated data forwarding from previous BS until we update the agents.
FLOOD - Bad, since it may take a long time for the gateway router to be notified.
HAWAII - good, since we forward traffic from previous BS.
MCAST - very good, since data is already present at the new BS.

3) Wired Bandwidth Overhead (control)

Control overhead high as updates could travel long distances for MIP (HA could be far away).
Control overhead high for FLOOD (flooding)
Control overhead good for HFA (FA at gateway is updated)
Control overhead good for MCAST (Local updates, but multiple BS in group)
Control overhead very good for HAWAII (truly local updates)

4) Wired Bandwidth Overhead (data)

Data overhead very high for MCAST (multiple BS's receive data all the time).
Data overhead for HAWAII should be low (especially, if we can locate optimal cross-over points. If Frame Selection (FS) is used, wired bandwidth overhead will increase for all the schemes except MCAST where we are perpetually in FS mode).
Data overhead for FLOOD, MIP, HFA should be low (default routing algorithm will result in good paths from HA to MS).

5) Router processing overhead (control)

HAWAII - to be evaluated. Basically, the cost of processing IP packets with options. Expect to be reasonable.
FLOOD - high overhead (a lot of control messages).
MCAST, HFA - low overhead.
MIP - updates could traverse long distance links.

6) Router processing overhead (data)

To be evaluated for HAWAII,FLOOD - could be reasonably high as we have to maintain host-based routing entries.
For MIP, decapsulation only at base-station - should be low overhead.
For HFA, decapsulation at multiple FA's - reasonable overhead.
For MCAST - no overhead (fast path).

7) Base Station processing overhead (control)

HAWAII - to be evaluated. Should be reasonably low (No FA support).
MIP,HFA - FA support.
FLOOD - a lot of extra updates which were flooded by other BS's.
MCAST - Need to join multicast groups for MS in neighboring BS's also.

8) Base Station processing overhead (data)

HAWAII - minimal. No FA support.
MIP, HFA - Decapsulation by the FA.
FLOOD - no overhead.
MCAST - process and drop data of MS in neighboring BS's.

9) Multipath forwarding

MIP,HFA,FLOOD,MCAST - no problem since they use standard routing protocols.

HAWAII - need to send out updates along multiple paths (multicast) during registration and handoff

10) Router failures

MIP,HFA, FLOOD, MCAST - standard routing protocols will take care of failures.
HAWAII - need to send out updates of host-entry routes along new paths. Also need to ensure that enough information is available in the surviving routers to recreate new paths.

11) FA failure

HAWAII,FLOOD - FA in MS - so wouldn't affect other MS's (assuming we don't use alternative 1).
FA failure in MIP is equivalent to BS failure (which impacts all schemes).
FA failure impacts HFA which has multiple FA's.
FA failure impacts MCAST (assuming alternative 1 is used).

12) IP address depletion

Directly corelated with FA presence in the network.
Thus, problems for HAWAII, FLOOD. No problem for MCAST, HFA, MIP.

13) Signaling message loss

HAWAII - use acknowledgements for registration/handoff.
MIP,HFA,FLOOD,MCAST - use acks.

14) Security

HAWAII - can use key based schemes (store code in current BS, transfer it to next BS when MS is authenticated using the secret key it supplies).

MIP,HFA,FLOOD,MCAST - standard procedures.

15) Multicasting support

Since all of these schemes are based on Mobile IP, use standard MobileIP techniques (for example, two-way tunnelling to HA)

16) Looping/Fast movement

MIP,HFA,FLOOD,MCAST - uses standard routing protocols.
HAWAII - loops should be detected at the BS and eliminated.

17) QoS support

Assuming that QoS support is difficult with encapsulated (tunneled) traffic since there is no way to distinguish two MS's attached to same BS. Thus, I have Good for HAWAII, FLOOD, MCAST and Bad for MIP and HFA. Of course, guaranteeing QoS support is still a difficult problem in the presence of mobility. I am assuming some sort of differentiated services type of scheme works.

May 10th '98

Hawaii testbed

(i) Connect 4 PC's to OmniView Belkin keyboard/mouse/monitor controller so that one console controls 4 PC's. Do this for another set of 4 PC's

(ii) Install Windows 95 by following Dell's setup

(iii) Install Ethernet cards on the machines as per the following testbed diagram

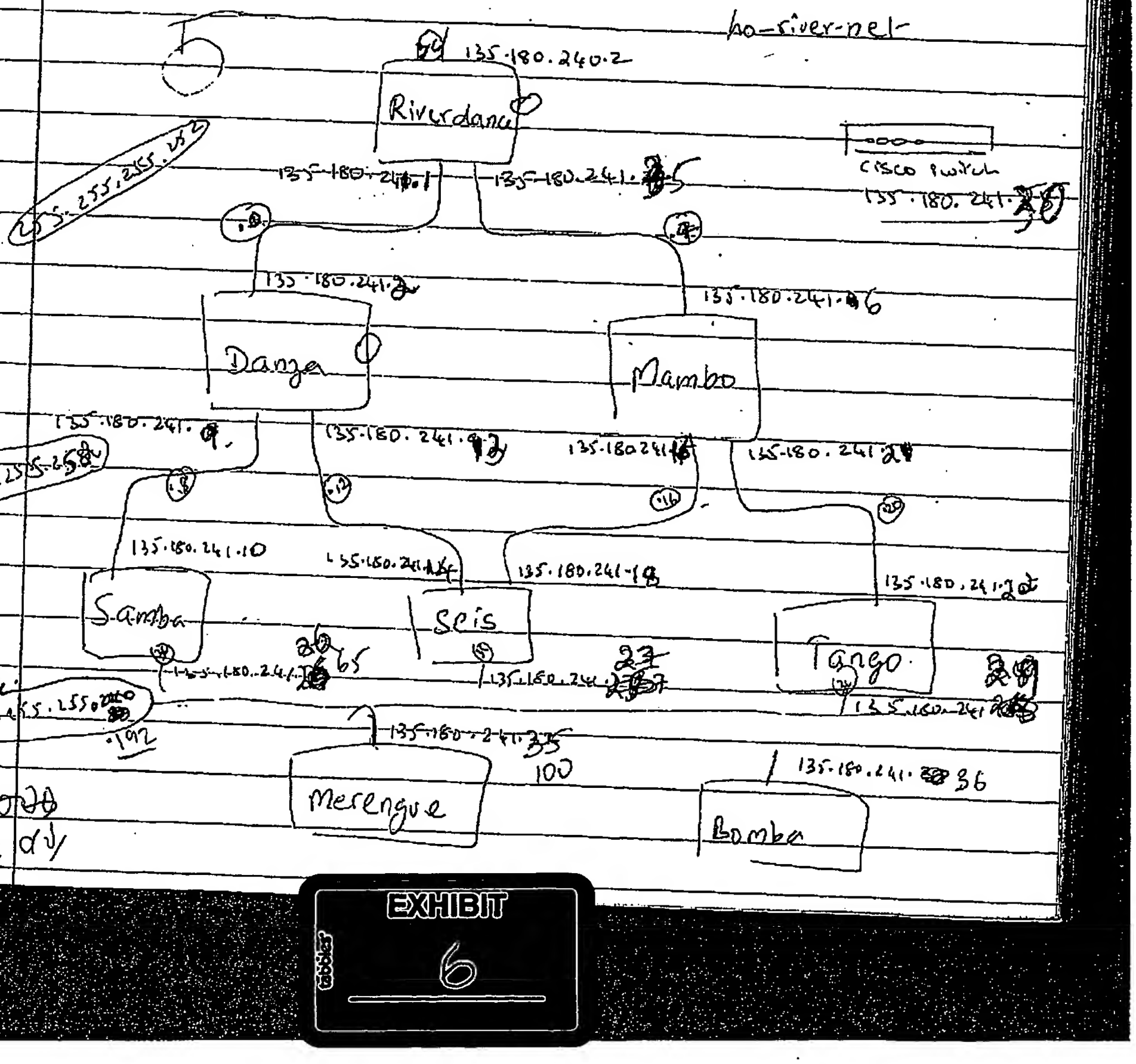
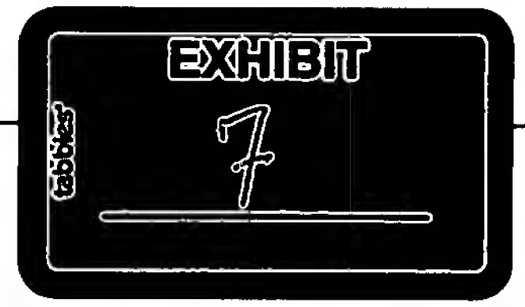


EXHIBIT 6

```
\documentstyle[times,epsf,12pt,myhdr]{article}

\setlength{\textheight}{8.75in}
\setlength{\columnsep}{2.0pc}
\setlength{\textwidth}{6.8in}
\setlength{\footheight}{0.0in}
\setlength{\topmargin}{0.25in}
\setlength{\headheight}{0.0in}
\setlength{\headsep}{0.0in}
\setlength{\oddsidemargin}{-.19in}
\setlength{\parindent}{1pc}

\idrawdir{/home/ramjee/hawaii/doc/fig}
\figdir{/home/ramjee/hawaii/doc/fig}

%\setcounter{page}{0}
%\baselineskip = 30 pt
%\lineskip = 30 pt
%\parskip = 14 pt
%\topmargin=-.3in
%\oddsidemargin = 0in
%\evensidemargin=0in
%\textwidth=6.4in
%\textheight=8.8in
%\parskip 4pt plus 1pt

\title{HAWAII: A Domain-based Approach for Supporting Mobility in
                Wide-area Wireless networks}

\author{}

\date{}


\begin{document}

\maketitle

\abstract{}

\ls{2.0}


\section{Introduction}

MobileIP is the current standard for supporting macro-mobility in IP
networks-\cite{Perk96}. MobileIP provides a good framework for
allowing users to roam outside their home networks without causing
disruption to their applications. However, it is not intended, and
thus does not perform well, for supporting micro-mobility (handoffs)
of mobile users. Recently, Route Optimization extension for MobileIP
with support for micro-mobility was proposed-\cite{Perk97}.  In this
proposal, packets are forwarded from the old base-station foreign
agent to the new base-station foreign agent to reduce disruption
during handoff.  However, the mobile device's care-of-address still
changes as the user moves between neighboring base-stations. This
results in undesirable notifications to the home agent and correspondent
hosts on every handoff of the mobile user.

Many of the proposals for supporting mobility have operated on the
assumption that there would be no special support available for
mobility in the infrastruture-\cite{Ches96}. We question the validity
of this assumption. Today's wide-area IP network is divided into
domains which are managed by independent entities. These entities
operate their own independent protocols within their domain while
agreeing upon a standard protocol when interacting between
domains. The division of routing protocols into intra-domain routing
protocols such as RIP-\cite{Malk94} or OSPF-\cite{Moy91} and
inter-domain routing protocols such as BGP-\cite{Loug91} is a classic
```



```
example of this domain-based management approach. Recently, there has
been a similar trend in the Quality of Service (QoS) community where
approaches that use Differentiated Services-\cite{Nich98} across
domains and Integrated Services-\cite{Shen97) within domains are being
proposed.

We observe that user mobility between base-stations is a localized
phenonmenon. Furthermore, user mobility is intrinsically tied to
routing of packets which has been a basic IP network service.  Thus,
we argue that a domain-based approach is well-suited for supporting
micro-mobility. When the handoff occurs between two base-stations
within the same domain, the domain-based approach would manage the
handoffs. When the handoff occurs between base-stations
that are connected to two different domains, we advocate using a
standard protocol such as MobileIP. In this way, handoff between
base-stations can be made transparent to the mobile user's home agent
and correspondent hosts as far as possible.

In this paper, we present the design, implementation, and performance
evaluation of Handoff-Aware Wireless Access Internet Infrastructure
(HAWAII). In HAWAII, the wired access portion of the wireless network
is divided into domains. As the mobile users move about within a
domain, the mobile device's IP address (\it remains unchanged}. The
home agent and the correspondent hosts of the mobile user are shielded
from the user's mobility in this domain. Packets are delivered to the
mobile device by specialized path setup schemes that update the
host-based routing tables in selective routers in the domain.  This is
in direct contrast to the Route Optimization proposal, where the
mobile device's care-of-address is changed on every move between
neighboring base-stations while the routing entries in the routers
remain unchanged. We also demonstrate that the HAWAII approach results
in quantitative gains (such as less disruption to user traffic during
handoff) as well as qualitative gains (ease of QoS support).


The remainder of the paper is organized as follows. In
Section-\ref{sch), we present the design principles of HAWAII. In
Section-\ref{path), we present three path setup schemes for supporting
mobility under HAWAII. In Section-\ref{sim), we compare the
performance of HAWAII with the basic MobileIP scheme and the MobileIP
Route Optimization schemes. In Section-\ref{imp}, we present
experiences and results from our implementation of the HAWAII approach
on a testbed of PCs running as routers and base-stations. In
Section-\ref{qos), we illustrate how providing Quality of Service in
the wired portion of the network is simplified using the HAWAII
approach. In Section-\ref{dis), we discuss other issues. In
Section-\ref{rel), we discuss related work. In Section-\ref{con), we
present our conclusions.


\section{HAWAII}
\label{sch}

In this section, we outline the goals and design principles of HAWAII.

%Goals
%       Mobility Transparency
%       QoS
%       Routing Efficiency
%       Reliability
%
%Achieved through
%       Hierarchy through domains
%       Unique Care-of-address for each mobile
%       Path setup schemes
%       Soft state
%
%Problems
%       Scalability
```



```
%       IP address depletion
%
%Solutions
%       Dynamic IP address assignment (no permanent home-address)


\subsection{Design goals}

In a wide-area internetwork, a mobile user may be in contact with
several hosts that are geographically widespread. In the current
MobileIP standard with Route Optimization, these correspondent hosts
are notified every time the mobile user is handed off from one
base-station to another. This notification not only increases the
amount of control traffic generated, but also places an unnecessary
processing burden on a fixed host which may be providing services to
hundreds of fixed and mobile hosts. Therefore, our first design goal is to
provide some transparency in user mobility.

Recently, there has been tremendous interest in supporting QoS in the
Internet. Several ways of providing Differentiated~\cite{Nich98} and
Integrated services~\cite{Shen97,Wroc97} have been proposed.  Our
second design goal is to be able ''build-in'' support for QoS in the
mobility management schemes from the very beginning.  In the MobileIP
standard (when the colocated care-of address option is not used),
packets are tunneled from a home-agent to the mobile device's
base-station. Since several users could be attached to the same
base-station, it is difficult to provide QoS support without either
inspecting the inside of tunneled packets or through some complex
aggregation mechanism~\cite{Terz98}.  Another problem with the
MobileIP standard (with or without the colocated care-of address
option) arises when a user moves between base-stations.  In this case,
the user's care-of address changes.  This could result in a new
reservation along the entire path from the home-agent (or the
correspondent host) to the mobile host, even when most of the path
(especially through the backbone routers) remains unchanged.

Our third design goal is routing efficiency.  The route inefficiency
problem arises when the mobile user is away from his home
network. This problem manifests both at the global scale as well as at
the local domain scale. In MobileIP,, packets are sent by correspondent
hosts to the home agent which then tunnels these packets to the mobile
device. This two leg routing inefficiency at the global scale is
addressed by the Route Optimization proposal (or IPv6) to a certain
extent. However, it can be expected that it will take quite some time
before a large number of fixed hosts are upgraded.  At the local
domain scale, in the MobileIP Route optimization proposal, packets are
forwarded from the old base-station to the new base-station until the
home-agent and then the correspondent hosts are notified. Depending on
the round trip time to the home-agent and correspondent hosts from the
mobile user, packets may follow the inefficient path at the domain
scale resulting in disruption to user traffic. This may particularly
be noticeable, for example in the form of audio clicks, in the case of
interactive audio applications. Thus, at the domain scale also, we
would like to be able to switch to an efficient route as quickly as
possible.

Our final design goal is reliability. In the current approach, foreign
agents are vulnerable to failure. If there is a hierarchy of foreign
agents~\cite{Aziz94}, reliability mechanisms need to be designed to
ensure recovery of foreign agents in the presence of failures. In
HAWAII, we would like to leverage the fault tolerance mechanisms
present in the standard routing protocols to ensure reliability of
data delivery for mobile hosts.

\subsection{HAWAII design}

In order to achieve the design goals listed in the previous subsection,
we use the following design principles in HAWAII.
```



```
\subsubsection{Hierarchy}

A common approach that is adopted for providing mobility transparency
to correspondent hosts is by dividing networks into hierarchies. In
HAWAII, the wireless access network is divided into domains, and the
movement of users within a domain are shielded from the users outside
the domain. Each domain is still identified as a subnet, thus,
resulting in no change to the routing entries in backbone routers
outside the domain. We use special techniques within the domain,
described later, to maintain packet flow to/from the mobile user.

\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir domain.eps}
\caption{Hierarchy using domains}
\label{domfig}
\end{figure}

When the user moves across domains, we use the same approach used in
the MobileIP standard.  The network architecture is illustrated in
Figure~\ref{domfig}. Packets flow directly to the mobile user as long
as the user's movement is within the domain. If the user moves into a
new domain, the home agent at the root router in the home domain
starts encapsulating packets to the new location of the mobile
user. Thus, applications can continue to use the same IP address
without disruption.

\subsubsection{Unique Addressing}

In order to provide QoS to user's flows, routers along the path of the
packet flow need to be able to classify packets to use the reserved
resources. This classification is typically done using the header
fields in the data packet~\cite{Laks98,Srin98}. In HAWAII, packets
sent to the mobile device are uniquely identified by the packet's
destination address, which is the mobile device's home address or its
colocated care-of address. Thus, providing per-flow QoS is greatly
simplified. Compare this to the case where packets are tunnelled to a
care-of-address in the base-station. In this case, mapping flow level
QoS to the tunnels is fairly complicated~\cite{Terz98}.

Mobile users in HAWAII are assigned a dynamic IP address through a
Dynamic Host Configuration Protocol (DHCP) server. As the users move
between base-stations within the domain, their IP address (\it does
not change). Thus, users outside the domain do not perceive the user's
mobility.  Furthermore, reservations from the correspondent host
(and/or home agent) to the domain remain unchanged as long as the
mobile user stays within the domain.

In this approach, we need to allocate two IP addresses for each mobile
host (one in the home network and one in the roaming network). This
exacerbates the limited IP address availability problem. In
Section~\ref{dis}, we discuss an optimization that helps reduce the
number of extra addresses needed.


\subsubsection{Path Setup Schemes}

So far, we have assigned a unique address for each mobile device and
agreed to let the mobile device retain this address as long as the
mobile user remains within the domain.  In this context, maintaining
packet flow within the domain to the mobile device requires special
techniques for managing user mobility. When the mobile device is
powered up, a path setup message establishes host-based routing
entries for the mobile device's IP address in the routers in the
domain so that packets arriving at the domain root router can reach
the mobile device. When the mobile device is handed off, it sends a
path setup message that updates the host based routing entries for the
```

mobile device's IP address in selective routers to ensure that packets continue to reach the device after the handoff. The choice of when and which routers are updated constitute a particular path setup scheme. In Section-\ref{path}, we describe three such path setup schemes.

These path setup schemes can take advantage of the knowledge of the wireless network and/or mobile devices (for example, whether mobile devices can listen on multiple base-stations at the same time) for ensuring less/no disruption to packet flow, optimized for the given environment. We present detailed performance results highlighting the performance advantageous of different path setup schemes for different configurations in Section-\ref{sim}.

One important question in using host-based routing in the domain routers is scalability. However, note that the maximum number of routing entries in a router depends on the number of mobile users active within the domain. Typically, due to the limited wireless bandwidth spectrum available, a base-station can have only upto 100 users who are powered up. Since modern routers can support on the order of 10,000 entries easily, the size of the domain needs to be engineered to include approximately 100 base-stations. Since the coverage area of 100 base-stations is quite large (radius of $20\mbox{Km}^2$ to $500\mbox{Km}^2$ depending on metropolitan or rural location), the majority of user movement will be within a domain resulting in transparent mobility with respect to home agents and correspondent hosts. To summarize, the scalability problem is tackled in a two-fold manner: a) leveraging of the processing power of current routers to handle on the order of 10,000 routing entries, and b) appropriate sizing of the domain to limit the maximum number of routing entries. Note that the backbone routers still have only subnet-based routing entries.

\subsubsection{Soft-State}

The notion of ''soft-state'' was introduced in~\cite{Clar88}. It refers to state in the routers that needs to be constantly refereshed and would otherwise be lost automatically. This technique is particularly useful in HAWAII, where users movement result in path setup messages establishing host-based routing entries in some domain routers. By periodically refereshing the host-based routing entries, we can adapt to changes in routing due to faults, congestion etc. These refresh path setup messages, unlike the path setup messages sent by the mobile device on powerup or handoff, are sent from each base-station to the root router in the domain, for all the mobile hosts attached to the base-station. Thus, router/link failures are easily handled in HAWAII. Furthermore, absence of one or more foreign agents in the packet path to the mobile host also improves the reliability of data delivery to the mobile user.

The periodic messages are also aggregate messages since the base-station sends one message for all the mobile users attached to its wireless interface. Furthermore, as we shall see in Section-\ref{path}, these update messages are sent to only a selected few routers in the domain. Thus, there is very little overhead associated with maintaining soft-state. Signaling protocols such as RSVP~\cite{Zhan93} also use the notion of soft-state and periodically refresh state information in the routers. Thus, reservation allocations can be combined with path setup messages in the HAWAII scheme, thereby deriving the benefits of RSVP-like soft-state.

\section{Path Setup Schemes in HAWAII}
\label{path}

In this section, we describe three path setup schemes that manage packet delivery to the mobile user. As mentioned earlier, there are two types of path setup messages. One is simply a refresh message to maintain the soft state routing entries. This is sent by the

base-station to the domain root router and is common to all the three schemes considered in this paper. The second type is an update path setup message sent by the mobile host during power up and handoff. This message updates routing table entries in the mobile device's base-station and selective routers in the domain. The three schemes differ only on how these updates are coordinated and maintained.

The refresh path setup message is not acknowledged. Loss of the refresh message is tolerated by making the soft-state routing entries timeout only when several consecutive refresh path setup messages are lost. The update path setup messages in all the path setup schemes are acknowledged and retransmitted if the message or the acknowledgement is lost. Thus, the path setup schemes are robust from path setup message loss.

Note that the three path setup schemes considered in this paper do not assume any topological knowledge. In other words, the path setup messages are routed in the domain using the routing entries created by regular routing protocols such as RIP~\cite{Malk94} or OSPF~\cite{Moy91} without using any additional information. One can envision more complex path setup schemes in the future where the path setup messages are routed based on current congestion levels or success of QoS availability along the route chosen.

\subsection{Path Setup Message Format}

The path setup message Information Element has six fields as shown in column 1 of Table-\ref{tab1}. Column 2 lists the values for these fields for the refresh path setup message sent by the base-station. Note that a refresh path setup message would contain multiple such Information Elements in one path seutp message, each Information Element representing one mobile device attached to the base-station. An update path setup message would contain only one such Information Element. In addition, all path setup messages could contain an authentication header to verify the authenticity of the message.

```
\begin{table}
\centering
\caption{Path Setup Message Information Element and the Refresh
Message}
\label{tab1}
\vspace*{.4cm}
\begin{tabular}{|l|l|}
\hline
Parameter & Refresh Path Setup Message\\
\hline
Message Type & Refresh\\
Sequence Number & Min(1,Sequence Number of the entry in base-station)\\
Mobile IP address & IP Address of mobile device attached to base-station\\
Source IP address & IP address of base-station sending the refresh message\\
Destination IP address & IP address of domain root router\\
Metric & set as one by base-station, incremented by others\\
\hline
\end{tabular}
\end{table}
```

The detailed operation and use of each of the fields in the update path setup messages is explained in the next two subsections.

\subsection{Path Setup Message after Power Up}

Consider the case when a mobile device is powered up. The mobile device is first assigned an IP address through the DHCP server. Lets assume that the DHCP server is located at the domain root router. Then, the base-station acts as a DHCP relay, forwarding the DHCP messages from the mobile user to/from the DHCP server. Upon successful authentication, the DHCP server assigns an IP address for

```
the mobile device and also informs the mobile device of the
base-station's and domain root router's IP addresses.

The mobile device then sends a path setup message with the fields as
listed in Table~\ref{tab2} to its current base-station.

\begin{table}
\centering
\caption{Power up Update Path Setup Message Information Element}
\label{tab2}
\vspace*{.4cm}
\begin{tabular}{|l|l|}
\hline
Parameter & Power up Update Path Setup Message\\
\hline
Message Type & Update\\
Sequence Number & zero \\
Mobile IP address & IP Address of mobile device\\
Source IP address & IP address of current base-station\\
Destination IP address & IP address of domain root router\\
Metric & set to zero by mobile device, incremented by others\\
\hline
\end{tabular}
\end{table}


\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir path0.eps}
\caption{Path Setup Message after Power Up}
\label{path0fig}
\end{figure}

When the current base-station receives the path setup message, as
illustrated in Figure~\ref{path0fig}, it increments the metric, adds a
routing entry for the mobile device with the outgoing interface as the
interface on which it receives the message (the wireless interface in
this case).  It then performs a routing table lookup to locate the
gateway (Router 1) for forwarding this entry to the destination IP
address in the message, i.e., the domain root router. The message is
forwarded to Router 1 (shown as message 2 in
Figure~\ref{path0fig}). Router 1 performs similar processing,
increments the metric, adds an entry for the mobile user, and forwards
the message to the domain root router. The domain root router adds an
entry for the mobile user and sends an acknowledgement back to the
mobile user (shown as message 4 in Figure~\ref{path0fig}). At this
time, packets destined for the mobile user arrive at the domain root
router based on the subnet portion of the mobile device's IP address.
The packets are then routed within the domain to the mobile device,
using the host-based routing entries just setup. Note that other routers
in the domain have no knowledge of the mobile device's IP address. These
routers would use a default route to the domain root router if they
recive a packet destined for the mobile device.


\subsection{Path Setup Message during Handoff}

In this subsection, we will describe the operations of the three path
setup schemes when the mobile user is handed off from one base-station
to another. Let us define the cross-over router as the router at the
intersection of two paths, one between the domain router and the old
base-station and another between the old base-station and the new
base-station.  In all the schemes considered below, routing entries
during handoff are added so that packets are forwarded from the old
base-station or the cross-over router to the new base-station. This
property insures us against the possibility of loop formation.
```



```
In all the three schemes, the mobile device then sends a path setup
message with the fields set as listed in Table~\ref{tab3} (except that
the source and Destination IP addresses are interchanged in the
Old-to-New scheme).  The schemes differ in how they interpret and act
using these fields.

\begin{table}
\centering
\caption{Handoff Update Path Setup Message Information Element)
\label{tab3}
\vspace*{.4cm}
\begin{tabular}{|l|l|}
\hline
Parameter & Handoff Update Path Setup Message\\
\hline
Message Type & Update\\
Sequence Number & Min((Sequence number of previous update + 1)\%MaxSeqNum, 2)\\
Mobile IP address & IP Address of mobile device\\
Source IP address & IP address of new base-station\\
Destination IP address & IP address of old base-station\\
Metric & set to zero by mobile device, incremented by others\\
\hline
\end{tabular}
\end{table}


We now describe the three path setup schemes in detail.

\subsubsection{New-to-Old Path Setup Scheme}


As the name of the path setup scheme indicates, a path setup message
is sent by the mobile device during handoff from the new base-station
to the old base-station. The base-station or routers that receive this
message update their routing entries for the mobile hosts to point to
the router/base-station from which the path setup message arrived. The
path setup message's final destination is the old base-station which
then acknowledges the message to the mobile device.

\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir path1.eps}
\caption{Path Setup Scheme:New-to-Old}
\label{path1fig}
\end{figure}

This scheme is illustrated in Figure~\ref{path1fig}. The path setup
message is first sent by the mobile device to the new base-station.
The new base-station adds a routing entry for the mobile device's IP
address with the outgoing interface as the interface on which it
received this message. It then performs a routing table lookup for the
old base-station's address and determines the forwarding router,
Router 1. The new base-station then forwards the path setup message to
Router 1 (shown as message 2 in Figure~\ref{path1fig}). The router
performs similar actions. It first adds a routing entry for the mobile
device's IP address with the outgoing interface as the interface on
which it received this message (since it already had an entry, it
simply changes the entry to use the new outgoing interface). The
router then forwards the path setup message to the old base-station
(shown as message 3 in Figure~\ref{path1fig}). The old base-station
changes its routing entry, redirecting packets to the mobile user back
on the wired network. The old base-station then sends an
acknowledgement of the path setup message back to the mobile user
(shown as message 4 in Figure~\ref{path1fig}). Note that only the new
and old base-stations and the routers connecting them are involved in
processing the path setup message. Other routers in the domain simply
have a default entry pointing to the domain root router, and remain
```

unchanged.

One important point to note is the need for sequence numbers in the path setup message. Recall that the base-stations periodically send referesh path setup messages to the domain root router. Consider the case in Figure~\ref{path1fig} when path setup message 2 is processed by the cross-over router. Imagine if the old base-station (which has not yet been notified of the handoff) now sends its periodic refresh. This refresh would indicate that the mobile device is still at the old base-station. If this refresh is now processed at the Router 1, the router would then change (back) its routing entry for the mobile device to point towards the old base-station. By now, the old base-station would have received the message 3 shown in Figure~\ref{path1fig} and would change its entry to redirect packets destined for the mobile device back to Router 1. This results in packets looping between the old base-station and Router 1 (until the next refresh comes from the new base-station).

This situation is avoided by having the mobile device increment the sequence number in its path setup message on every handoff. The path refresh messages would always contain the sequence number stored with the routing entry (received on the most recent handoff). In the aforementioned case, the refresh message that arrives at Router 1 would have a lower sequence number than the routing entry created by path setup message sent by the mobile device. Thus, the router would simply forward the refresh message without changing its routing entry thereby avoiding the undesirable looping.

A sequence number of zero, sent only during power up, is treated as a special case and always processed. This is to ensure packet delivery if the mobile device resets itself (for example, due to battery failure). In order to handle this special case, we also make sure that all refresh messages (which normally contain the sequence number present in the routing entry) have a minimum sequence number of one. Also, the sequence numbers of path setup messages generated after every handoff by the mobile device is always incremented by one in a wrap around fashion between two and the maximum sequence number.

```
\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir path1-2.eps}
\caption{Path Setup Scheme:New-to-Old}
\label{path1-2fig}.
\end{figure}
```

In Figure~\ref{path1fig}, the router connecting the two base-stations turns out to also be the cross-over router. If the topology is such that the two base-stations are directly connected as shown in Figure~\ref{path1-2fig}, packets would get forwarded from the old base-station to the new base-station after the exchange of the path setup messages 1-3 during handoff. Assuming the cost of route is based on hop count, this path setup message would result in non-optimal routing since packets from the domain root router would be forwared to Router 1, the old base-station and then the new base-station rather than to the new base-station directly from Router 1. This non-optimality is easily corrected when the new base-station sends out a refresh path setup message to the domain root router. This refresh path setup message would follow the most cost efficient route to the root router (shown by messages 4 and 5 in Figure~\ref{path1-2fig}). This will create routing entry updates such that packets would now start flowing from the root router to Router 1 to the new base-station, resulting in optimal routing. The soft-state routing entry in the old base-station would automatically timeout when path setup refreshes for the mobile device no longer reach the old base-station.

Now consider the case when there is a link failure on the link connecting the new base-station to Router 1 in Figure~\ref{path1-2fig}. The refresh path setup message would now proceed from the new base-station to the root router through the old base-station. This is because the routing protocols would detect the link failure and would automatically select the old base-station as the gateway for the next best route from the new base-station to the root router. In this way the flow of packets to the mobile would be restored.

\subsubsection{Old-to-New Path Setup Scheme}

This scheme is very similar to the New-to-Old path setup scheme. One difference is, as the name implies, a path setup message is sent by the mobile device first to the old base-station, which then sends the message to the new base-station. Another difference is the metric is set by the old base-station to one more than the metric found in its routing table for the new base-station and then decremented as the message goes along.

```
\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir path2.eps}
\caption{Path Setup Scheme:Old-to-New}
\label{path2fig}
\end{figure}
```

This scheme is illustrated in Figure~\ref{path2fig}. The first message sent by the mobile device is addressed to the old base-station. The message is shown directed towards the new base-station because, depending on the wireless conditions, the wireless link to the old base-station could be highly error prone or even broken. If the link to the old base-station is still functioning, this message could be directed to the old base-station. In any case, the old base-station processes this path setup message and updates its routing entry for the mobile device. It then determines the gateway for forwarding the packet to the new base-station and forwards the path setup message to Router 1 (shown as message 2 in Figure~\ref{path2fig}). Router 1 updates its routing entry for the mobile device and then forwards the entry to the new base-station. The new base-station adds an entry for the mobile device and then finally forwards the path setup message back to the mobile device.

\subsubsection{New-to-Old-to-New Path Setup Scheme}

This scheme is more complex than the previous two path setup schemes. This scheme involves a more descriptive routing table in the routers. A routing table typically has an entry of the form (IP address -> outgoing interface). In this scheme, we require the routing table to be able to route based on another field, the incoming interface of the packet. In other words, the routing entry is of the form (incoming interface, IP address -> outgoing interface). Note that the format of the {\it forwarding tables} on the interface ports in the router is still the same. While in the original case, all the interface ports had the same forwarding entries for a given IP address, we now could have different forwarding entries for a given IP address on different interface ports.

```
\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir path3.eps}
\caption{Path Setup Scheme:New-to-Old-to-New}
```

```
\label{path3fig}
\end{figure}


This scheme is illustrated in Figure-\ref{path3fig}.  In this scheme,
as a path setup message is sent from the new to the old base-station,
there are two cases. If there is no existing entry for the mobile
host's IP address, a regular entry for the mobile hosts is added to
point to the router/base-station from which the path setup message
arrived. For example, the new base-station and Router 2 in
Figure-\ref{path3fig} simply adds an entry of the form (*,IP->Intf B).


If there exists an entry for the mobile host's IP address, then the
router adds an entry of the form (interface to which the path setup
message will be forwarded, mobile host IP address -> interface on
which the path setup message arrived). The router also modifies its
original entry (\it to exclude) from its input interface, the
interface on which the message will be forwarded. For example, in
Figure-\ref{path3fig}, the domain root router adds an entry (Intf
B,IP->Intf C) and changes its original entry (*,IP->Intf B) to
($\neg$Intf B,IP->Intf C).

The final destination of the message, the old base-station adds a
regular entry to forward the mobile host's packets to the interface on
which it received the path setup message.


Now, the second phase of the path setup scheme begins. The old
base-station sends a path setup message back to the mobile device.
When this message arrives at the routers with entries of the form
($\neg$Intf2,IP->Intf2) and (Intf2,IP->Intf1), they simply replace these
entries with (*,IP->Intf1). For example, Router 1 and the domain root
router perform this action after messages 6 and 7 respectively.  If a
router (e.g. Router 2) has only one entry of the form (*,IP
addr->Intf), then it simply forwards the packet. The packet finally
arrives at the new base-station and the path setup scheme is complete.

\section{Simulation results}
\label{sim}

{\bf Note: Working on it. Need to get Shieyuan to run a few more
simulations.}

\subsection{Overlapping cells, soft handoff}

\subsection{Overlapping cells, hard handoff}

\subsection{Non-overlapping cells}

\section{Implementation results}
\label{imp}

{\bf Note: Myself and Kannan are redesigning the HAWAII implementation
to be independent of the routing protocol. Therefore, I have just
given a brief sketch here of the current implementation which is
integrated with routed (RIP).}

\subsection{Path Setup Schemes}

The path setup schemes were implemented by extending version 2 of
the Routing Information Protocol (RIPv2). The format of the path setup
message is shown in Figure-\ref{messagefig}.

\begin{figure}[htpb]
\centering
\leavevmode
\setlength{\epsfxsize}{0.65\textwidth}
\epsffile{\Idrawdir message.eps}
```



```
\caption{Path Setup Scheme: Message Format}
\label{messagefig}
\end{figure}


We describe the implementation of the New-to-Old path setup scheme.
The implementation of other schemes is similar.

The processing at a node proceeds as follows.  A typical RIPv2 update
message has a family field identifier as AF\_INET. The path setup
messages in HAWAII use the family identifier as AF\_MOBINET to
distinguish it from the routing update messages. Among the path
setup messages, the refresh path setup messages have the command field
as RIPCMD\_RESPONSE while the update path setup messages have  the
command field as RIPCMD\_RESPONSE\_ACK.

When the routing daemon receives a RIP message with the family
identifier AF\_MOBINET, it increments the metric field and adds an
entry of the form (mobile host's IP address->Interface on which this
message was received). If the routing daemon already has an entry for
the mobile host, it updates the entry if the sequence number of the
message is either zero or greater\footnote{Sequence number comparison
is done while taking wraparound of sequence numbers into effect.} than
the sequence number in the original entry. The routing daemon then
determines the interface on which the message is to be forwarded by
using the routing table entry for the destination address field in the
message and then forwards the message to the next hop router. If the
next hop address is the same as one of the interface addresses of the
current router/base-station, the path setup message has reached its
final destination. In this case, an acknowledgement is generated if
the command field is RIP\_RESPONSE\_ACK (for the update path setup
message).  The acknowledgement is sent to the mobile host. If authentication
information is maintained in the base-station, then the
acknowledgement containing the authentication information is first sent to
the new base-station (address in the source address field) which then
forwards the acknowledgement to the mobile host.

\subsection{Integrating DHCP, MobileIP and RIP}

When the mobile device is powered up, it first sends a DHCP DISCOVER
message to the base-station. The base-station acts as a DHCP relay and
forwards this message to the DHCP server. The DHCP server replies to
the mobile device with a DHCP OFFER message. The mobile host then
sends a DHCP REQUEST message to the base-station which relays the
message to the DHCP server. The DHCP server sends back a DHCP RESPONSE
which contains the mobile host's assigned address (the 'ciaddr'
field), the base-station's address (the 'giaddr' field) and the domain
root router's address (the 'siaddr' field).

The mobile host now sends an update path setup message to the current
base-station with a sequence number of zero and with the final
destination as the domain root router. This message establishes
routing entries in selective routers in the domain so that packets
arriving at the domain root router can be delivered to the mobile
host. When the mobile host is handed off to a new base-station in the
same domain, it updates its sequence number as specified in
Section~\ref{path} and sends a path setup message using the New-to-Old
scheme to maintain connectivity after handoff. These path setup
messages are processed as described in the previous section.

If the mobile host is handed off to a new base-station in a different
domain, the mobile host acquires a care-of address using DHCP in the
new domain. It then informs its home agent in the previous domain with
its new care-of address. Packets are then tunneled to/from the
home-agent as long as the mobile host remains in the new domain. When
the mobile host is powered down, it relinquishes the DHCP address
leases on both the original and the new domain.

\section{QoS}
```

IP address through DHCP in the new domain. This address becomes the mobile device's colocated care-of address. The mobile device still retains its original IP address assigned in its home network, and packets are tunneled to/from a home agent in its home network to its current location. When the device is powered down, it gives back its assigned addresses (permanent address and care-of address, if any). On the next power up, the device gets assigned a new permanent address in that domain.

This is similar to the ''dialup model'' of service provided by Internet Service Providers to fixed hosts. The difference is that the users in HAWAII are mobile and the home domain is determined by where the device is powered up rather than which modem access number is dialed. Apart from requiring fewer IP addresses, this optimization also solves the triangular routing problem if the user does not move out of a domain while powered up. A disadvantage of this approach is if the mobile device would like to advertize a fixed name, for example, when the mobile device serves as a web server. One could envision extending Domain Name Service(DNS) with dynamic address mapping to support this service or assign fixed permanent addresses as is done in MobileIP for those specific users.

An interesting question arises when we consider the ''sleep'' mode used by laptops. Do we maintain the laptop's IP address in order to preserve applications such as telnet? If the answer is yes, then how do we track the user as he moves? One solution to this problem is to allow the device to retain its IP address and do a 'page' operation, similar to the paging in cellular networks, to locate the user if a packet is to be delivered to him. When the device ''wakes-up'', it would need to register again with the network.

\section{Related Work}
\label{rel}

MobileIP is the standard for supporting basic mobility in IP networks. Several proposals based on extending MobileIP to support micro-mobility have been proposed recently-\cite{Aziz94,Bala95,Cace96,Perk97,Sesh96}.

\section{Conclusion}
\label{con}

\begin{thebibliography}{999}

\bibitem{Aziz94} A. Aziz, ''A Scalable and Efficient Intra-Domain Tunneling Mobile-IP Scheme,'' ACM Computer Communication Review, Vol. 24, No. 1, Jan 1994.

\bibitem{Bala95} H. Balakrishnan, S. Seshan, and R.H. Katz, ''Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks,'' ACM Wireless Networks, 1(4), Dec. 1995.

\bibitem{Cace96} R. Caceres and V.N. Padmanabhan, ''Fast and Scalable Handoffs for Wireless Internetworks,'' in ACM Mobicom, Rye, New York, Nov. 1996.

\bibitem{Ches96} S. Cheshire and M. Baker, "Internet Mobility 4x4," Proceedings of SIGCOMM'96, August 1996.

\bibitem{Clar88} D. Clark, ''The Design Philosophy of the DARPA Internet Protocols,'' in the Proceedings of ACM SIGCOMM'88.

\bibitem{Laks98} T.V. Lakshman and D. Stiliadis, ''High Speed Policy-based Packet Forwarding Using Efficient Multi-dimensional Range Matching,'' in the Proceedings of ACM SIGCOMM'98.

\bibitem{Loug91} K. Lougheed and Y. Rekhter, ''A Border Gateway

Protocol 3 (BGP-3),'' Request for Comments 1267, October 1991.

\bibitem{Malk94} G. Malkin, ''RIP Version 2 Carrying Additional Information,'' Request for Comments 1723, November 1994.

\bibitem{Moy91} J. Moy, ''OSPF Version 2,'' Request for Comments 1247, July 1991.

\bibitem{Nich98} K. Nichols and S. Blake, ''Differentiated Services Operational Model and Definitions,'' Internet Draft, Feb 1998.

\bibitem{Perk96} C.E. Perkins, ''IP Mobility Support,'' Request for Comments 2002, October 1996.

\bibitem{Perk97} C.E. Perkins, D.B. Johnson, ''Router Optimization in Mobile IP,'' Internet Draft-work in progress, November 1997.

%\bibitem{Salt84} J. Saltzer, D. Reed, and D. Clark, ''End-To-End %Arguments in System Design,'' ACM Transactions on Computer Systems, %Vol. 2, No. 4, 1984.

\bibitem{Sesh96} S. Seshan, H. Balakrishnan, and R.H. Katz, ''Handoffs in cellular wireless networks: The Daedalus implementation and experience,'' Kluwer International Journal on Wireless Communication Systems, 1996.

\bibitem{Shen97} S. Shenker, C. Partridge, and R. Guerin, ''Specification of guaranteed quality of service,'' Request for Comments 2212, September 1997.

\bibitem{Srin98} V. Srinivasan, G. Varghese, S. Suri, and M. Waldvogel, ''Fast Scalable Algorithms for Level Four Switching,'' in the Proceedings of ACM SIGCOMM'98.

\bibitem{Terz98} A. Terzis, L. Zhang, E. Hahne, '' Reservations for aggregate traffic: experiences from an RSVP Tunnels Implementation,'' International Workshop on QoS, IWQoS, 1998.

\bibitem{Wroc97} J. Wroclawski, ''Specification of the controlled-load network element service,'' Request for Comments 2211, September 1997.

\bibitem{Zhan93} L. Zhang, S. Deering, D. Estrin, S. Shenker, and D. Zappala, ''RSVP: A New Resource ReSerVation Protocol,'' IEEE Network Magazine, September 1993.

%Mobile-IP Local Registration with Hierarchical Foreign Agents, % C. Perkins, Internet Draft, Feb 1996.

\end{thebibliography}

\end{document}

```
\label{qos}

{\bf Sandy: would you like to write a brief summary of our QoS
approach?}

\section{Discussion}
\label{dis}

In this section, we discuss other issues are pertinent to HAWAII.

\subsection{Security}

We need to be careful to disallow arbitrary users from sending path
setup messages and thereby subverting somebody else's traffic. The
path setup messages considered in this paper are secure because they
all require the old base-station to cooperate.  Authentication
information for the user is first stored in the current base-station
when the mobile user powers up. When the mobile host is handed off to
a new base-station, the old base-station approves of the path setup
message only if the mobile host is able to authenticate itself in the
path setup message.  The authentication information is then
transferred from the user's old base-station to the new base-station
on the acknowledgement of the path setup message.

The assignment of IP address during the user's power up registration
also needs to be secured to prevent arbitrary users from acquiring IP
addresses. This can be achieved either using a mechanism such as Home
Location Register (HLR) authentication as is done in today's cellular
networks or using the RADIUS protocol authentication mechanism.

\subsection{Tunnneling}

When the mobile device is away from its home network, packets are
typically tunneled from the home-agent to the mobile device. If the
correspondent hosts implement route optimization, then packets can be
delivered directly to the mobile device. However, it will be a while
before the correspondent hosts are upgraded. Tunneling packets by the
home agent involves adding an additional header in each of the packets
sent to the mobile host. This additional header can have some
undesirable side-effects as shown in the tcpdump trace in
Figure~\ref{fig:tcpdump1}, with CH as the correspondent host, MH as
the mobile host, HA as the home agent and FA as the foreign agent.



\textfigure{tcpdump1}{TCPDUMP trace that shows tunneling side-effects}
{
1) CH.40102 > MH.commplex-link: S 1626551371:1626551371(0) \\
\ix win 8760 <mss 1460> (DF) (ttl 255, id 47691)\\
2) HA > FA: CH.40102 > MH.commplex-link: S 1626551371:1626551371(0)\\
\ix win 8760 <mss 1460> (DF) (ttl 254, id 47691) (DF) (ttl 254, id 51069) \\
3)  MH.commplex-link > CH.40102: S 3552498482:3552498482(0) ack 1626551372\\
\ix win 17520 <mss 1460> (DF) (ttl 63, id 6624) \\
4) CH.40102 > MH.commplex-link: . ack 3552498483 win 8760(DF) (ttl 255, id 47692
)\\
5) HA > FA: CH.40102 > MH.commplex-link: . ack 3552498483 win 8760 (DF)\\
\ix (ttl 254, id 47692) (DF) (ttl 254, id 51070)\\
6) CH.40102 > MH.commplex-link: P 1:1461(1460) ack 1 win 8760 (DF) (ttl 255, id
47693)\\
7) HA > CH: icmp: MH unreachable - need to frag (mtu 1480) (DF) (ttl 255, id 510
72)\\
8) CH.40102 > MH.commplex-link: . 1:1441(1440) ack1 win 10080 (DF) (ttl 255, id
47694)\\
9) HA > FA: CH.40102 > MH.commplex-link: . 1:1441(1440) ack 1 win 10080 (DF)\\
\ix (ttl 254, id 47694) (DF) (ttl 254, id 51078) \\
10) MH.commplex-link > CH.40102: . ack 1441 win 17520 (DF) (ttl 63, id 6627) \\
}
```



```
The first five steps in Figure~ref{fig:tcpdump1} show the TCP handshake
(through the HA) and determination of the maximum segment size (mss)
as 1460. However, in step 6, when the first packet with a payload of
1460 is sent with the Don't Fragment flag set (path MTU discovery),
the HA returns an icmp error message back to the CH since adding
tunnel headers would require fragmentation. After step 7, the new path
MTU of 1440 is used. Thus, the tunneling header has an undesirable
side-effect of an additional one round trip wastage between the
correspondent host and the home agent. This can be especially
noticeable in the case of web transfer from a mobile host where each
web page could have multiple tcp downloads.

The tunneled packet has an outer header with HA:FA as the source and
destination addresses and an inner header with CH:MH as the source
and destination addresses. In the case of HAWAII, since we use a
colocated care-of address, we could instead perform as a swap
operation. That is, when the packet arrives with the header as CH:MH
at the home agent, the home agent simply changes the destination
address to FA. Thus packets leaving the home agent would have a header
of CH:FA and would incur no additional overhead. When the packet
reaches the mobile host, the colocated foreign agent would then swap
back the CH:FA header to CH:MH and pass it on to the application. This
swap operation incurs no header overhead and works whenever the
foreign agent is colocated with the mobile device. We have implemented
this option as an extension to the home agent and foreign agent
functionality in MobileIP. A trace of tcpdump when this option is used
is shown in Figure~\ref{fig:tcpdump2}.

\textfigure{tcpdump2}{TCPDUMP trace that shows SWAP in operation}
{
1) CH.50704 > MH.rfe: S 2197768393:2197768393(0) win 8760 <mss 1460> (DF)\\
2) CH.50704 > FA.rfe: S 2197768393:2197768393(0) win 8760 <mss 1460> (DF)\\
3) MH.rfe > CH.50704: S 4212372961:4212372961(0) ack 2197768394 win 17520 <mss 1
460> (DF)\\
4) CH.50704 > MH.rfe: . ack 1 win 8760 (DF)\\
5) CH.50704 > FA.rfe: . ack 4212372962 win 8760 (DF)\\
6) CH.50704 > MH.rfe: P 1:1461(1460) ack 1 win 8760 (DF)\\
7) CH.50704 > FA.rfe: P 0:1460(1460) ack 1 win 8760 (DF)\\
8) MH.rfe > CH.50704: . ack 1461 win 17520 (DF)\\
}

The first five steps in Figure~\ref{fig:tcpdump2} is again the TCP
handshake. Note that step 2 and step 5 are generated by the home agent
even though the source address is that of the correspondent host. As
can be seen in steps 6 through 8, there is no icmp 'need to fragment'
error messages as no additional header is added.

One drawback of using this option is that the packets leaving the home
agent with a header of CH:FA would have a topologically incorrect
address if the correspondent host does not belong to the same domain
as the home agent. In this case, packets leaving the home agent could
be dropped by ingress-filtering routers that try to prevent source
address spoofing. The same problem also exists in today's MobileIP
when the mobile host transmits packets with its home address in a
foreign domain. In HAWAII, this option can be only used if the home
and visiting domains are connected by a network where ingress
filtering is not deployed.

\subsection{Dynamic Permanent Address}

Recall that we need to allocate two IP addresses for each mobile host
(one in the home network and one in the roaming network). This
exacerbates the limited IP address availability problem.  One
optimization that we advocate to address this problem is the notion of
``dynamic permanent addressess''. In other words, mobile devices do
not have permanent addresses. As the mobile device is powered up in a
domain, it is assigned its permanent address through DHCP. This domain
also becomes the moible device's home domain. If the mobile device
moves into a different domain while powered up, it is assigned another
```